TECHNOLOGY & SECURITY

| Kai Sedgwick (https://news.bitcoin.com/author/kaisedgwick/) |

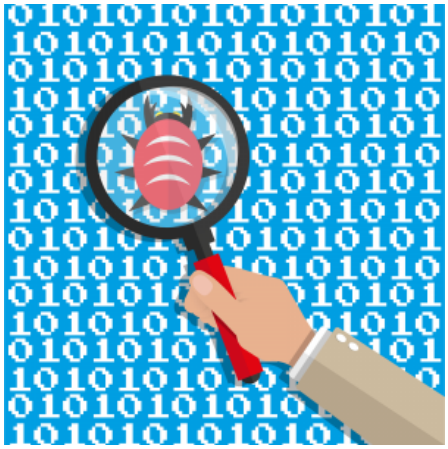
Report Claims 34,000 Ethereum Smart Contracts Are Vulnerable to Bugs

(https://news.bitcoin.com/wp-content/uploads/2018/02/bad-code-smart-contract.jpg)

Over 34,000 ethereum smart contracts containing $4.4 million in ETH may be vulnerable to exploitation. That's the conclusion reached by a quintet of researchers hailing from Singapore and the UK. Their technical report, which is currently

Also read: *Bad Code Has Lost $500 Million of Cryptocurrency in Under a Year (https://news.bitcoin.com/bad-code-has-lost-500-million-of-cryptocurrency-in-under-a-year/)*

Smart Contracts Are Only as Smart as Their Creator



"Finding The Greedy, Prodigal, and Suicidal Contracts at Scale" is the provocative title of a research paper (https://arxiv.org/pdf/1802.06038.pdf) submitted by British and Singaporean students last week. Its authors have dived deep into ethereum smart contracts, "finding contracts that either lock funds indefinitely, leak them carelessly to arbitrary users, or can be killed by anyone". This latter flaw is precisely what happened to Parity last November.

The dangers of relying on smart contracts that have not been independently audited are well-documented. In the past year, $500 million has been lost due to bad code, and around half of that figure involved ethereum. The most notorious case was the Parity bug which led to $168 million of ether being rendered permanently inaccessible, though there have been plenty of smaller incidents where inexperienced or inattentive developers have been caught out.

A Small Drop in a Big Ocean

The authors of the report claim to have used a tool to analyze almost one million smart contracts, of which 34,200 were found to be vulnerable, with 2,365 of these stemming from distinct projects. That means that around 3.4% of all smart contracts are potentially vulnerable to being hacked, broken, or otherwise exploited. Of the contracts that the research team flagged as being exploitable, "the maximal amount of Ether that could have been withdrawn...is nearly 4,905 Ether" worth $4.4 million.

dollars) have been sent to dead contracts after they have been killed." One thing the report deliberately omits is the identity of the smart contracts flagged as being at risk. But with almost 1 in 20 contracts vulnerable, and a jackpot of over $4.5 million in ether up for grabs, determined attackers have every incentive to put this research to the test.

What do you think can be done to make smart contracts safer? Let us know in the comments section below.

Images courtesy of Shutterstock.

Need to calculate your bitcoin holdings? Check our tools (http://tools.bitcoin.com/) section.

(https://news.bitcoin.com/author/kaisedgwick/)

Kai Sedgwick (https://news.bitcoin.com/author/kaisedgwick/)

Kai's been playing with words for a living since 2009 and bought his first bitcoin at $19. It's long gone. He's previously written white papers for blockchain startups and is especially interested in P2P exchanges and DNMs.

(https://twitter.com/bitcoin101)